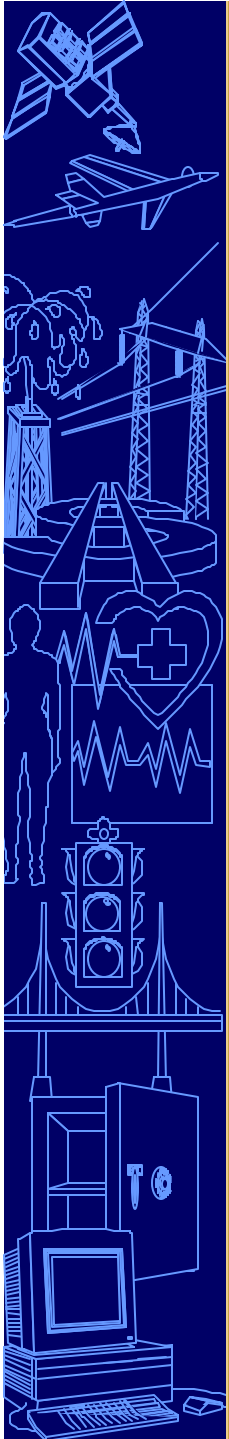


National Critical Infrastructure Protection A Case for Action

PCIE CIPP Review

Washington, D.C.

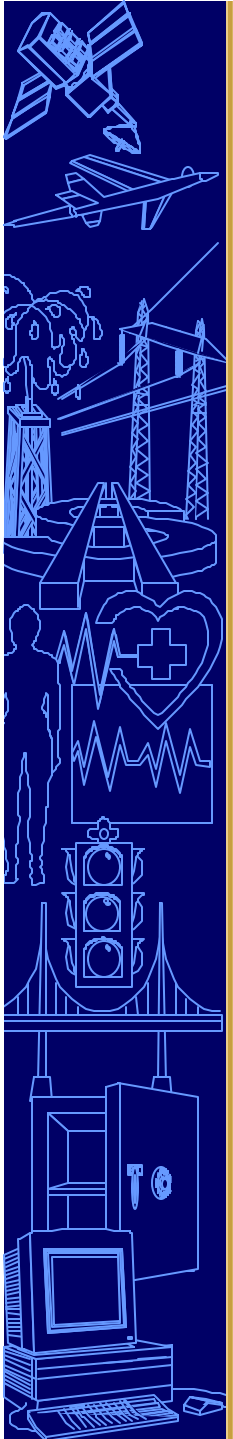
November 17, 1999



Critical Infrastructures

Federal Government's Concerns

- 4 **Assure government services including economic security**
- 4 **Assure national defense capability: logistical and war-fighting**
- 4 **Defend against new dimension of warfare/terrorism**
- 4 **Dependency of all the above on private industry owned and operated infrastructures and services**



Change Converging

4 New “geography”

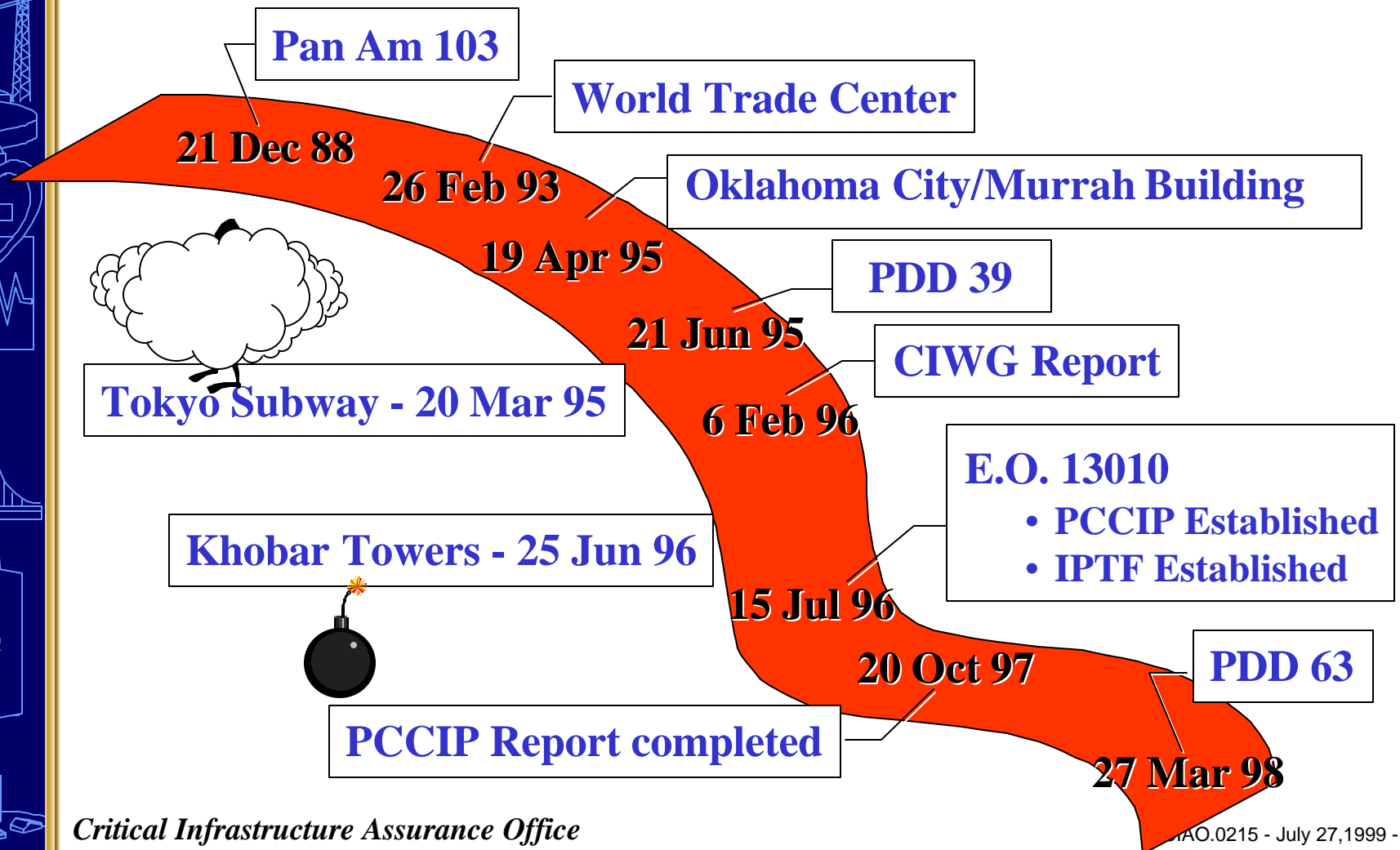
- Cold war ends; no longer bipolar world – multi polar
- No new nationalistic wars; growth of terrorism
- Global interdependence; international economic orders
 - e.g. banking and finance are global
 - e.g. distribution and supply channels
- Information and infrastructure are targets as never before

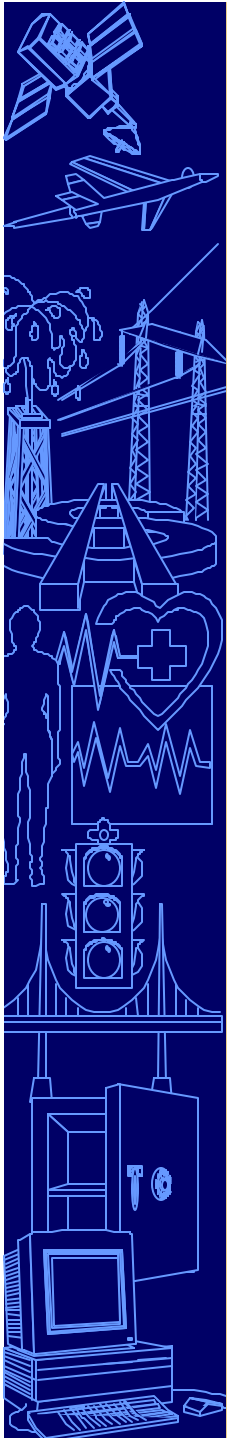
4 New dimension: Comprehensive dependence on information systems in the Information Age

4 National security = national defense + economic competitiveness

4 Shared use of critical infrastructures

Events Sequence





Information Age Threat Spectrum

National Security Threats	Info Warrior	Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage
	National Intelligence	Information for Political, Military, Economic Advantage
Shared Threats	Terrorist	Visibility, Publicity, Chaos, Political Change
	Industrial Espionage	Competitive Advantage Intimidation
	Organized Crime	Revenge, Retribution, Financial Gain, Institutional Change
Local Threats	Institutional Hacker	Monetary Gain Thrill, Challenge, Prestige
	Recreational Hacker	Thrill, Challenge

**I
N
S
I
D
E
R
S**

Computer-Based Security Threats

With *Intention* to Do Harm

Techniques	Infrastructure Target	Impact
------------	-----------------------	--------

<ul style="list-style-type: none">• Access• Penetration• Alteration		
---	--	--

	<ul style="list-style-type: none">• Information• Communications	
--	--	--

		<ul style="list-style-type: none">• Disrupt• Deny• Destroy• Steal
--	--	--

- The tools, expertise, capability and delivery mechanisms *are available and accessible*;
- The only trigger needed is a malicious intent, with a will and motivation to disrupt, deny, destroy or steal.



Presidential Decision Directive 63

4 **PCCIP Report October 1997**

4 **PDD 63, May 1998**

4 **Key initiatives for both physical and cyber dimensions:**

- Foster partnerships
- Education & awareness
- Information sharing; indications and warning
- Risk assessment
- Research & development
- Mitigating legal and other obstacles
- Government as a role model

U.S. Dependence on Information Technology

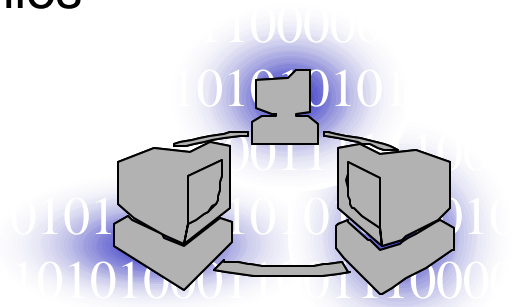
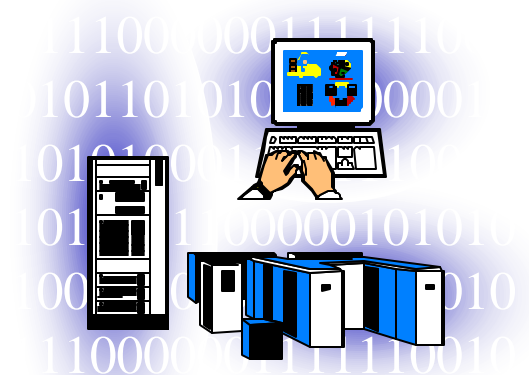
4 **\$730 billion/year industry;**

4 **The U.S. uses:**

- 42% of the world's computing power
- 60% of the world's Internet assets
- 200 million connect hours/day
- 170 million telephone access lines

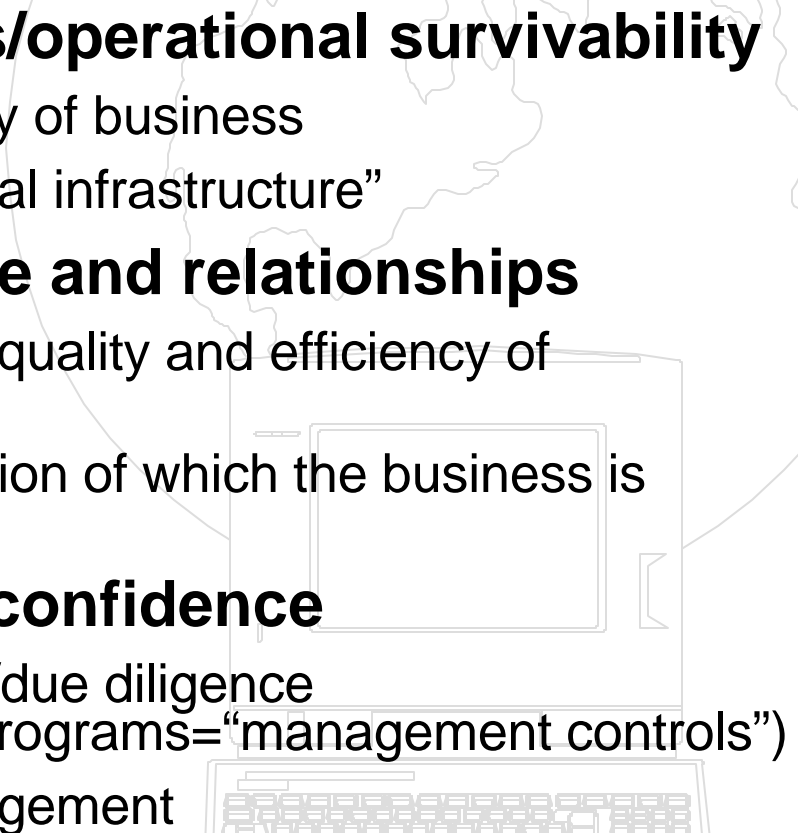
4 **The U.S. has reshaped business and government:**

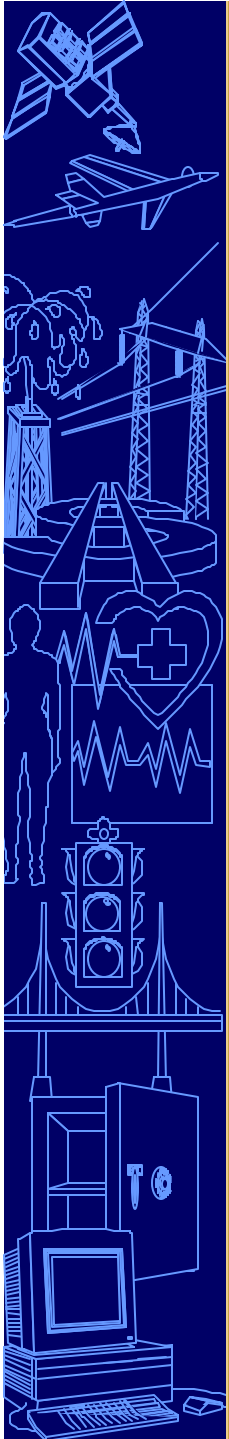
- 90% of large and 75% of small companies have LAN's
- 14 million faxes are connected
- 2 billion miles of fiber optic and copper cable provide data and voice services





Private Industry **Consequential Business Issues**

- 
- 4 **Business operations/operational survivability**
 - Disruption and integrity of business
 - Contribution to “national infrastructure”
 - 4 **Customer confidence and relationships**
 - Meet expectations for quality and efficiency of service/product
 - Protection for information of which the business is custodian
 - 4 **Public and Investor confidence**
 - Prudent management/due diligence (information security programs=“management controls”)
 - Liability and risk management



Federal Government:

A Services Delivery Institution

- 4 **Over 250 million “customers”**
- 4 **The public’s safety net**
 - E.g. Medicare and Medicaid funding to 67 million Americans,
 - E.g. Social Security benefits to 40 million people,
 - E.g. Veterans Affairs benefits to nearly two million families
- 4 **\$30-\$40 billion/year spent on information technology**



Federal Government: **Consequential Issues**

- 4 **More than industry, government is a “natural” target**
- 4 **Equivalent issues of:**
 - Reliability and integrity of services
 - Privacy
 - Public confidence and trust
- 4 **Additional issue of national security**



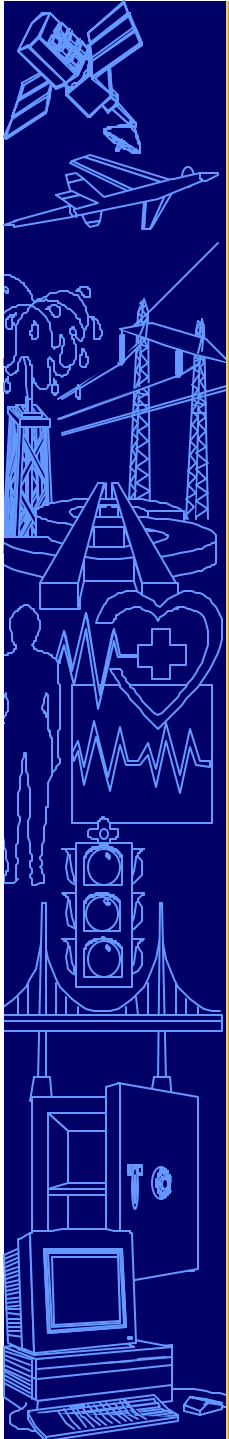
Scope of Attention

4 Two levels

- Strategic, including policy
- Tactical (operational)
- Tactical implementation requires strategic buy-in

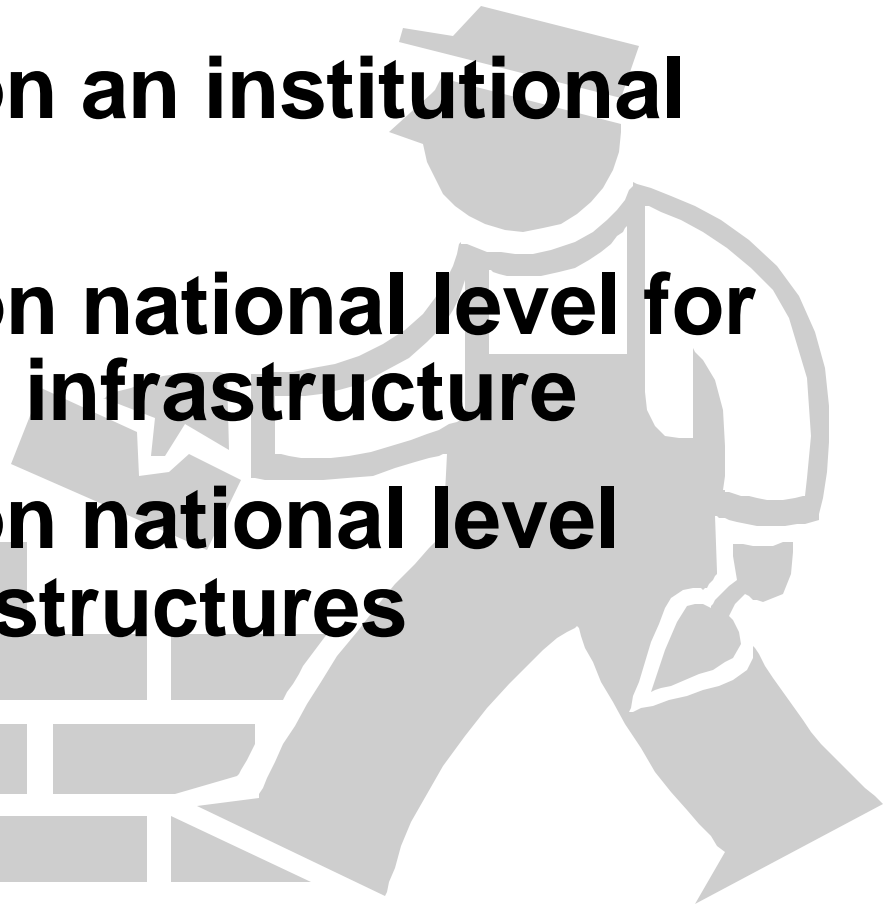
4 Mainstreaming the issue

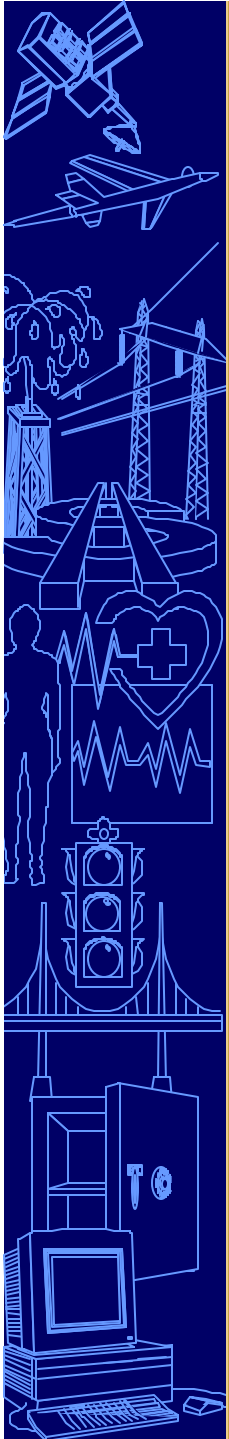




Layers of Action

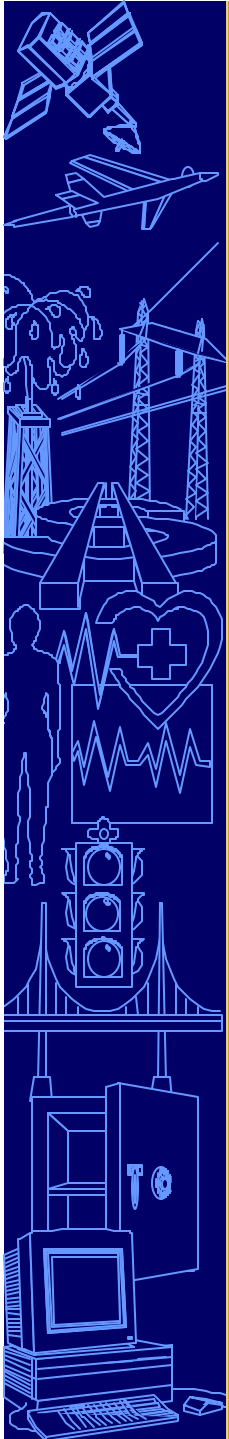
- 4 **Protection on an institutional level**
- 4 **Protection on national level for each critical infrastructure**
- 4 **Protection on national level across infrastructures**





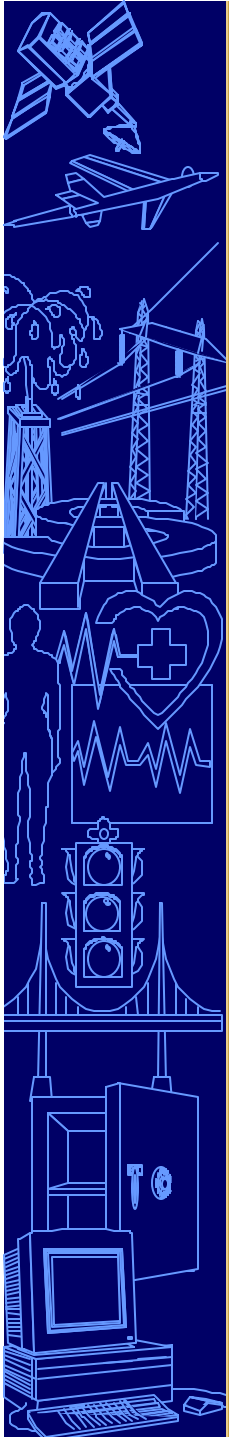
Audit Community and Risk Managers

- 4 Strategic professional community
- 4 Channel of communication and influence for policy and investments
- 4 Evolution of due diligence/prudent management
 - Business operational survivability
 - Customer relationships and obligations
 - Investor and public confidence
- 4 Compliance to “industry standards” and “generally accepted principles”



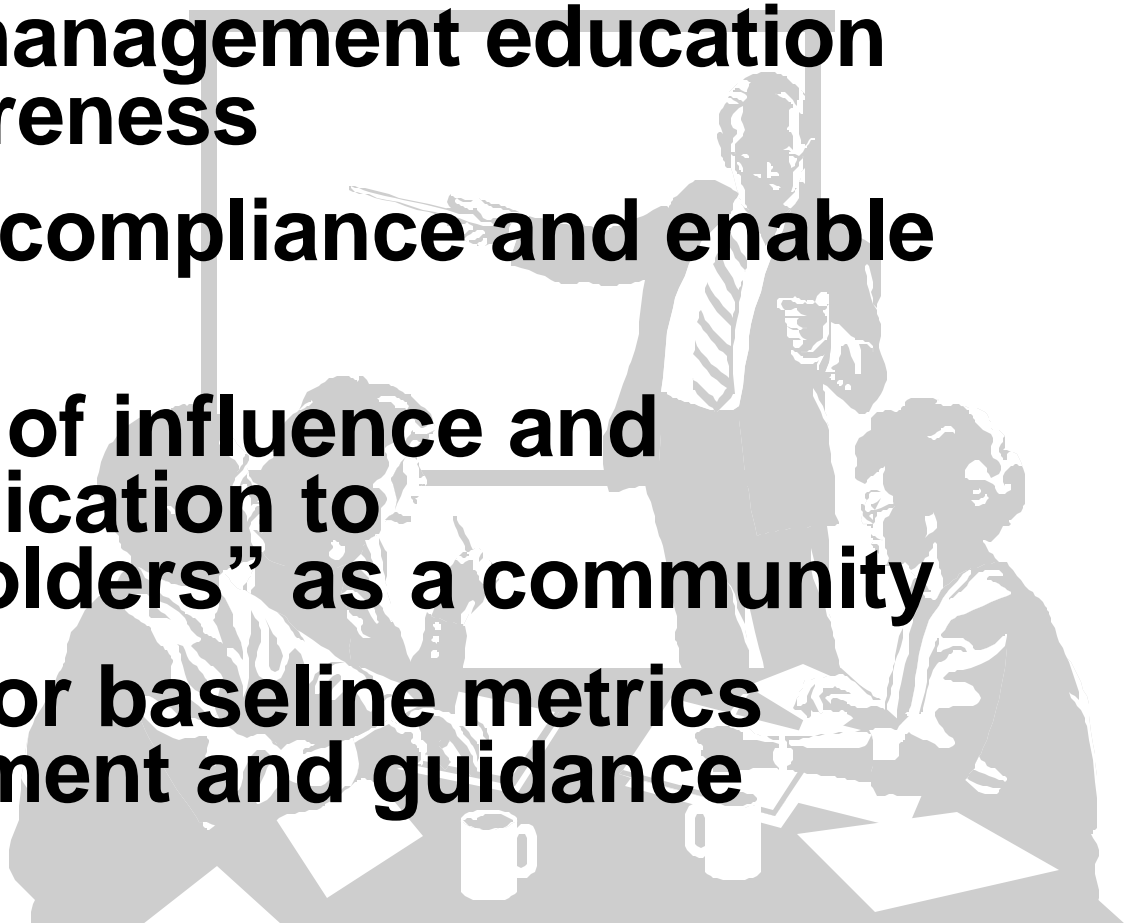
Audit Community Strategy

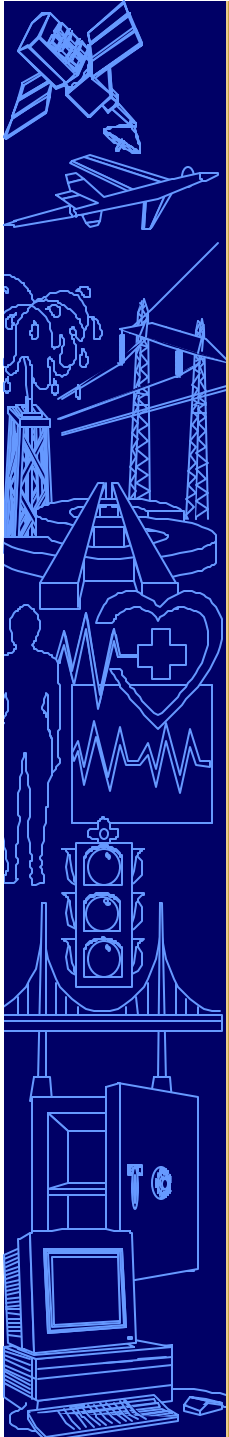
- 4 **Community collaboration: internal, external, IT auditors, the “big 5”**
- 4 **Senior management and board of directors education and awareness**
- 4 **Best practices, tools, standards, methodologies and guidance (evolution of roles and skills)**



IG Contribution

- 4 **Senior management education and awareness**
- 4 **Support compliance and enable action**
- 4 **Channel of influence and communication to “shareholders” as a community**
- 4 **Source for baseline metrics development and guidance**





PCIE CIPP Review Guideline

- 4 **Major first step**
- 4 **Elevates and sustains management attention and focus**
- 4 **“Big picture” perspective; reflects “national” character of the issue**
- 4 **Comprehensive review and progress assessment**